

Self Assessment Checkliste - Risikobewertung Internationaler Datentransfer nach Schrems II

Risikofaktoren (Beispiele)

		Auswirkung Risiko*
Risikohörende Faktoren / Maßnahmen	Risikofaktor „Zielland“	
	Kritisches Drittland wie bspw. USA, China, Russland, Mittlerer Osten (ggf. zukünftig auch UK)	
	Besondere Risiken für staatliche Zugriffe aufgrund nationaler Sicherheitsgesetze (z. B. FISA 702, EO 12333)	
	Eingeschränkte Rechtsschutzmöglichkeiten für EU-Betroffene	
	Risikofaktor „Dienstleister/Datenimporteur“	
	Telekommunikationsdiensteanbieter	
	Anbieter elektronischer Kommunikationsleistungen (E-Mail, Video, Messenger, etc.)	
	Cloud-Provider	
	Dienstleister/Datenimporteur war in der Vergangenheit bereits Adressat staatlicher Zugriffsmaßnahmen	
	Analyse-/Trackingdienstleister (z. B. Webseiten-Tracking)	
	Anbieter nachrangiger IT-Services (Wartung/Pflege, Support, etc.)	
	Gruppeninterner Datentransfer / Dienstleister	
	Risikofaktor „Art der Daten“	
	Besondere Kategorien personenbezogener Daten (Gesundheit, Religion, etc.)	
	Sensible Bank- und Finanzdaten	
	HR-Daten	
Bestandsdaten von Arbeitnehmern oder Endkunden (Kontaktdaten, E-Mail-Adresse, User-Name)		
Nutzungsdaten (LogIn-Daten, Webtracking-Daten, ohne Standortlokalisierung)		
Risikoreduzierende Faktoren / Maßnahmen	Standarddatenschutzklauseln mit erweiterten Verpflichtungen/Sicherungsmaßnahmen, insb. transparente Information und ggf. Genehmigung durch Datenexporteur bei behördlichen Zugriffen	
	Erweiterung Betroffenenrechte / Ausgleich Rechtsschutzdefizite	
	Compliance-Bestätigung Dienstleister	
	Zertifizierungen des Dienstleisters zu Datenschutz/Datensicherheit	
	Einbindung Betroffener - Einwilligungslösung	
	Binding Corporate Rules (BCR)	
	Verhaltensregeln/Code of Conducts	
	Beschränkung auf pseudonyme Daten / Tokenization	
	Datenlokalisierung EU/EWR (Container-Lösung, Treuhänder-Modell)	
	Verschlüsselungsmaßnahmen	
Sonstige technische oder organisatorische Sicherheitsvorkehrungen zur Einschränkung von Zugriffen		
* Legende Risikoauswirkung		
	- risikohörend -	- risikoneutral - Risiko vorhanden, aber nicht erhöht
		- risikoreduzierend -

Die Einstufung der Risikoauswirkungen erfolgt auf Grundlage von Best Practices und ohne Übernahme einer Haftung.